

Notice of Allowability	Application No.	Applicant(s)
	09/966,015	ZIMMER, VINCENT J.
	Examiner Jason Proctor	Art Unit 2123

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. This communication is responsive to Applicants' response submitted 30 January 2006.
2. The allowed claim(s) is/are 9, 11, 15, 17, 27, 29 and 37-40.
3. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All
 - b) Some*
 - c) None
 of the:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) hereto or 2) to Paper No./Mail Date _____.
 - (b) including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. Notice of References Cited (PTO-892)
2. Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date 1/30/06
4. Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. Notice of Informal Patent Application (PTO-152)
6. Interview Summary (PTO-413),
Paper No./Mail Date 20060403.
7. Examiner's Amendment/Comment
8. Examiner's Statement of Reasons for Allowance
9. Other _____.

EXAMINER'S AMENDMENT AND REASONS FOR ALLOWANCE

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Cory Claassen (50,296) on 31 March 2006.

The application has been amended as follows:

Claim 9, line 6, after the words "pre-boot phase of" delete the word "the" and insert the word --a--.

Claim 27, line 3, after the words "pre-boot phase of" delete the word "the" and insert the word --a--.

Claim 27, line 2, following the word "comprising:" insert the phrase --implementing an extensible firmware framework via which firmware modules are loaded during a pre-boot phase of a computer system;--.

2. The following is an examiner's statement of reasons for allowance:

Applicants' arguments submitted on 30 January 2006 have been fully considered and have been found persuasive. While the prior art of record teaches an extensible firmware

interface [“Extensible Firmware Interface Specification Version 1 .02” by Intel Corporation], using a VMM to emulate legacy hardware [US Patent No. 6,397,242 to Devine et al.], and authenticating firmware modules by comparing digital signatures [US Patent No. 5,844,986 to Davis et al.], these isolated teachings are insufficient to render the claimed invention obvious.

As suggested by Applicants’ arguments, in Devine, “Whatever authentication technique is used, the salient feature is that it is performed within the cryptographic coprocessor on the local version of the new BIOS program.” (column 4, lines 4-7). This teaching is distinct from the positively recited limitations of each independent claim.

Therefore, none of the references taken either alone or in combination with the prior art of record disclose a method or apparatus specifically including:

(Claim 9) implementing an extensible firmware framework via which firmware modules are loaded during a pre-boot phase of a computer system; implementing a firmware-based virtual machine monitor (VMM) upon the computer system; and authenticating, via the VMM, at least one of the firmware modules that is loaded during the pre-boot phase by comparing a digital signature provided with the at least one of the firmware modules with valid digital signatures stored in a secure storage that is accessible to the VMM, but which the VMM makes inaccessible to the firmware modules and the legacy code,

(Claim 15) the computer system including an extensible firmware framework via which firmware modules are loaded during a pre-boot phase of the computer system; and a virtual machine monitor (“VMM”) implemented thereon, the VMM further authenticating the firmware modules loaded during the pre-boot phase by comparing digital signatures provided with the

firmware modules with valid digital signatures stored in secure storage accessible to the VMM, but which the VMM makes inaccessible to the firmware modules,

(Claim 27) implementing an extensible firmware framework via which firmware modules are loaded during a pre-boot phase of a computer system; implementing a virtual machine monitor (VMM) during the pre-boot phase of the computer system; and authenticating a firmware module via the VMM by comparing a digital signature provided with the firmware module to the digital signatures in the secure storage,

in combination with the remaining elements and features of the claimed invention. It is for these reasons that Applicants' invention defines over the prior art of record.

Regarding the claim terminology, it is noted that "extensible firmware framework" is known in the art as defined by, for example, "Extensible Firmware Interface Specification Version 1.02" by Intel Corporation. Applicants' remarks make it clear that "authenticating, via a VMM" means authenticating with software, not hardware:

In contrast, independent claim 9 recites authenticating firmware modules with a VMM. A VMM is software—not hardware—and distinctly different from a cryptographic coprocessor. (Applicants' response 30 January 2006, page 7)

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

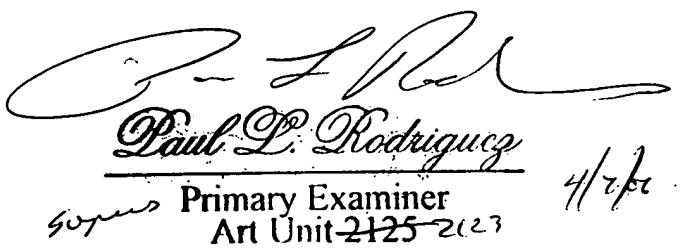
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason Proctor whose telephone number is (571) 272-3713. The examiner can normally be reached on 8:30 am-4:30 pm M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Paul Rodriguez can be reached at (571) 272-3753. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Any inquiry of a general nature or relating to the status of this application should be directed to the TC 2100 Group receptionist: 571-272-2100. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jason Proctor
Examiner
Art Unit 2123

jsp



Paul L. Rodriguez 4/7/01

Sovus Primary Examiner
Art Unit 2123